

MATHEMATICS PROBLEM 137

Chain addition is a technique employed in cryptography for extending a short sequence of digits, called the *seed* to a longer sequence of pseudorandom digits. Quoting David Kahn (in *Kahn on Codes*, MacMillan, New York, 1983, p. 154), "the first two digits of the [seed] are added together modulo 10 [which means they are added and the carry is neglected] and the result placed at the end of the [sequence], then the second and third digits are added and the sum placed at the end, and so forth, using also the newly generated digits when the [seed] is exhausted, until the desired length is obtained". Thus, the seed 3964 yields the sequence 3964250675632195... .

- a. Show that this sequence eventually repeats itself.
- b. Show that the sequence begins repeating itself with "3964".
- c. EXTRA CREDIT: How many digits are there before the first repetition of "3964"?

Each midshipman submitting a correct solution with a correct explanation to Problem 137 by 1700 Friday 12 March 2004 will be recognized as a solver on the next problem. Submit solutions to Prof. Wardlaw at mathprob@usna.edu (please no attachments!) or via his mailbox in Chauvenet 301.

Midshipmen Jordan Kehrer and Stephen McMath each submitted a correct solution to Mathematics Problem 136. A solution is on the back of this page and posted on the right wall at the Bancroft entrance to Chauvenet Hall.

MATHEMATICS PROBLEM 136

Show that the polynomial

$$p(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 4x^2 + 4x + 1$$

has no integer roots.

Solution

If x is an even integer, $p(x)$ is an odd integer, and if x is an odd integer, $p(x)$ is also an odd integer, so there is no integer x such that $p(x) = 0$.

The solvers both used the

Rational Roots Theorem. If $q(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is a polynomial with integer coefficients a_0, a_1, \dots, a_n and $q(r) = 0$ for some rational number $r = a/b$ where a and b are integers with $\gcd(a, b) = 1$, then a divides a_0 and b divides a_n .

It follows that if $r = a/b$ is a rational root of $p(x) = 0$ in lowest terms, then a and b both divide 1. Hence, $r = \pm 1$ is the only possibility. But $p(1) = 17$ and $p(-1) = -1$, so $p(x) = 0$ has no rational roots, and certainly no integer roots.